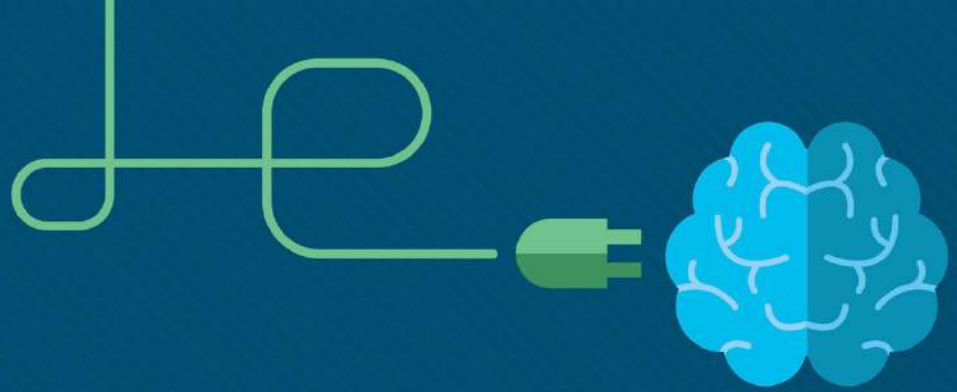


Capítulo 2: Ataques, conceitos e técnicas

Introdução ao Cybersecurity v2.1

2.1 Análise de um ataque cibernético

Encontrando vulnerabilidades de segurança

- Um *exploit* é o termo usado para descrever um programa escrito para tirar proveito de uma vulnerabilidade conhecida.
- Um *ataque* é o ato de usar um exploit contra uma vulnerabilidade.
- Vulnerabilidade de software
  - Erros no código do sistema operacional ou aplicativo
  - SYNful Knock – vulnerabilidade no Cisco IOS
    - permite que invasores obtenham o controle dos roteadores
    - monitorar a comunicação da rede
    - infectar outros dispositivos de rede.
  - Project Zero – Google formou uma equipe permanentemente dedicada a encontrar vulnerabilidades de software.

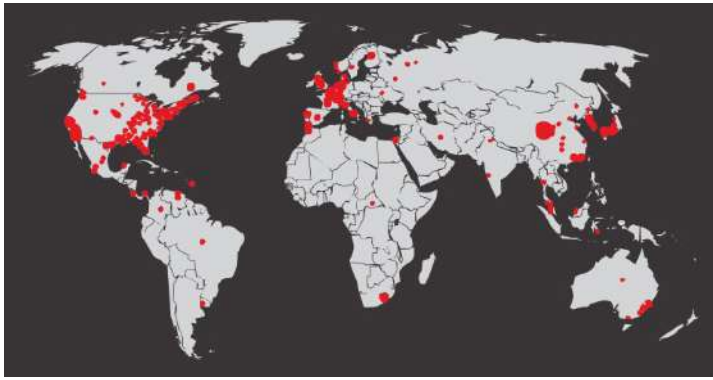
- Vulnerabilidade de hardware
  - Falhas de projeto de hardware
  - Rowhammer – exploit de memória RAM permite que os dados sejam recuperados das células de endereço de memória próximas.

Categorizar vulnerabilidades de segurança

- Buffer Overflow
  - Os dados são gravados além dos limites de um buffer
- Entrada não validada
  - Força os programas a se comportarem de forma não intencional
- Condição de corrida
  - Eventos indevidamente ordenados ou cronometrados
- Fragilidade nas práticas de segurança
  - Protege dados confidenciais através de autenticação, autorização e criptografia
- Problemas de controle de acesso
  - Controle de acesso a equipamentos físicos e a recursos
  - Práticas de segurança

Tipos de Malware

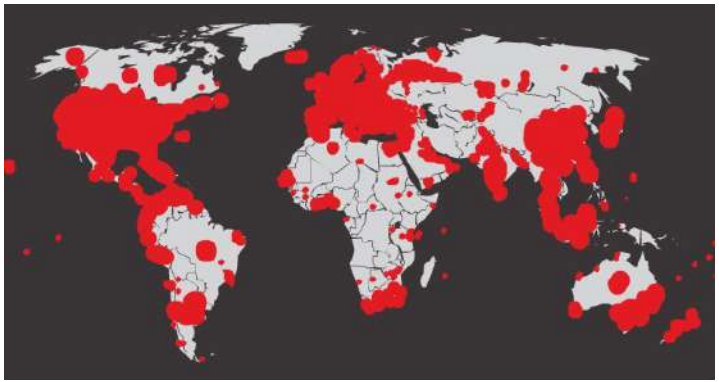
- O malware é usado para roubar dados, ignorar os controles de acesso, causar danos ou comprometer um sistema.
- Tipos de malware
  - **Spyware** – rastreia e espiona o usuário
  - **Adware** – entrega anúncios, geralmente vem com spyware
  - **Bot** – executa a ação automaticamente
  - **Ransomware** -mantém um sistema de computador, ou seus dados presos até que o pagamento seja feito
  - **Scareware** – persuade o usuário a executar uma ação específica por medo.



Infecção de worm de código vermelho inicial

Tipos de Malware (continuação)

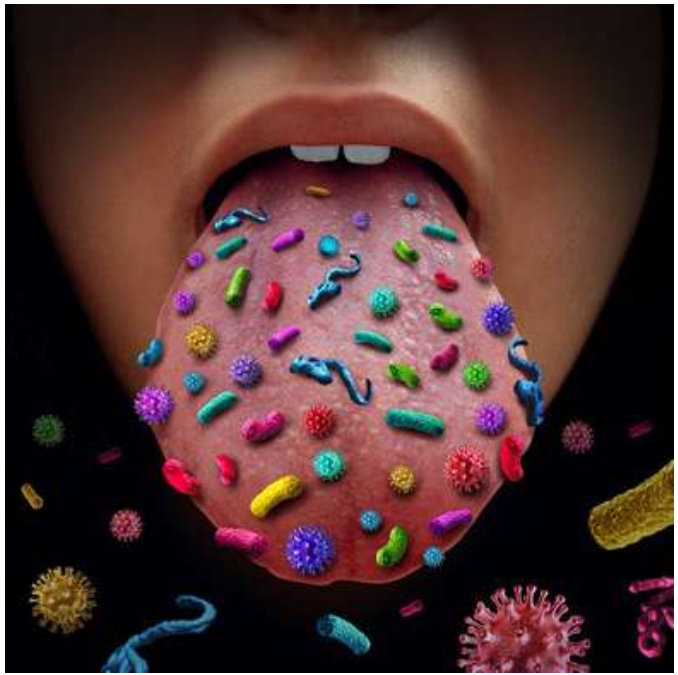
- Tipos de Malware (continuação)
  - **Rootkit** – modifica o sistema operacional para criar um backdoor
  - **Vírus** -código executável mal-intencionado anexado a outros arquivos executáveis
  - **Cavalo de Troia** – realiza operações mal-intencionadas disfarçadas de uma operação desejada.
  - **Worm** -replica-se explorando independentemente as vulnerabilidades nas redes
  - **Man-in-The-Middle** ou **Man-in-The-Mobile** – assume o controle sobre um dispositivo sem o conhecimento do usuário



Code Red Worm – Infecção pelo worm 19 horas depois

Sintomas de Malware

- Há um aumento no uso da CPU.
- Há uma diminuição na velocidade do computador.
- O computador congela ou trava frequentemente.
- Há uma diminuição na velocidade de navegação na Web.
- Existem problemas inexplicáveis com conexões de rede.
- Arquivos são modificados.
- Arquivos são excluídos.
- Há presença de arquivos, programas ou ícones de desktop desconhecidos.
- Há processos desconhecidos em execução.
- Programas estão se desligando ou reconfigurando sozinhos.
- E-mails estão sendo enviados sem o conhecimento ou consentimento do usuário.



Engenharia Social

- Engenharia social – manipulação do indivíduo para executar ações ou divulgar informações confidenciais
  - **Pretexting** – um invasor chama uma pessoa e mente para ela na tentativa de obter acesso a dados confidenciais.
  - **Tailgating** – Um invasor segue rapidamente uma pessoa que possui acesso a um local protegido.
  - **Something for Something (Quid pro quo)** – um invasor solicita informações pessoais de uma pessoa em troca de algo, como um presente.

Quebra de senha de acesso à rede WiFi

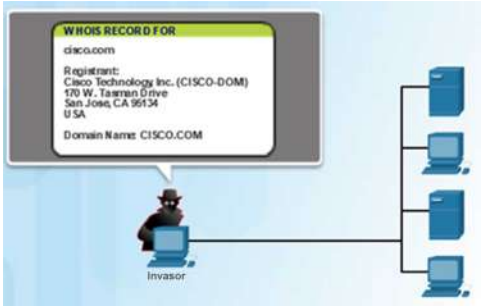
- Quebra de senha de acesso à rede WiFi – Descoberta de senha
  - **Engenharia social** – o invasor manipula uma pessoa que conhece a senha para fornecê-la.
  - **Ataques de força bruta** – o invasor tenta várias senhas possíveis na tentativa de adivinhar a correta.
  - **Sniffing de rede** – a senha pode ser descoberta ao ouvir e capturar pacotes enviados na rede.

Phishing

- Phishing
  - uma pessoa mal-intencionada envia um e-mail fraudulento, como sendo de uma origem legítima e confiável.
  - engana o destinatário para instalar o malware no dispositivo dele ou compartilhar informações pessoais ou financeiras.
- Spear phishing
  - um ataque de phishing altamente direcionado

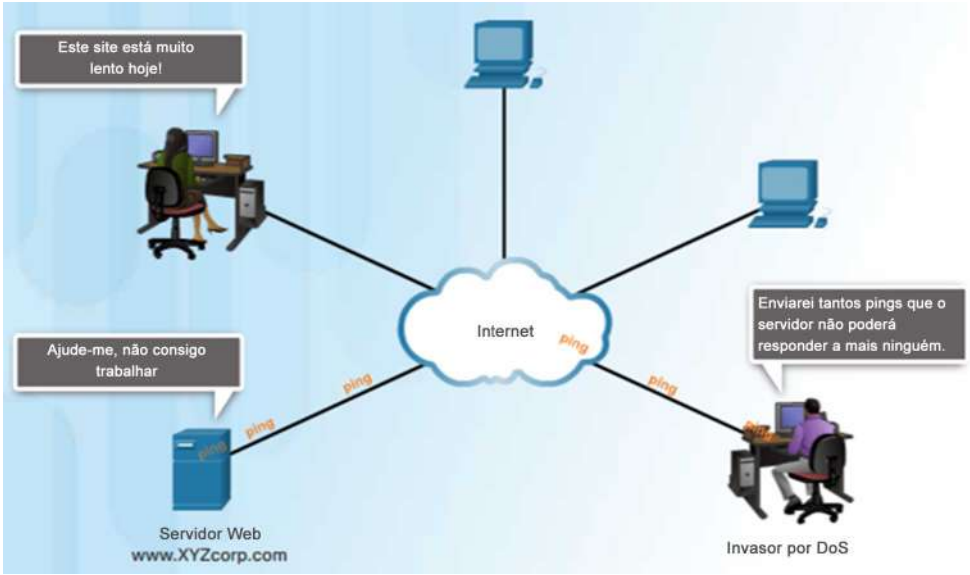
Exploração de vulnerabilidade

- Exploração de vulnerabilidade – varredura para encontrar a vulnerabilidade a ser explorada
  - **Etapa 1** – Reunir informações sobre o sistema de destino usando o scanner de porta ou engenharia social
  - **Etapa 2** – Determinar as informações aprendidas na Etapa 1
  - **Etapa 3** – Procurar vulnerabilidade
  - **Etapa 4** – Usar um exploit conhecido ou gravar um novo exploit
- Advanced Persistent Threat (APT) – uma operação multi-fase, longo prazo, furtiva e avançada contra um alvo específico
  - geralmente bem financiada
  - implanta o malware personalizado



DoS

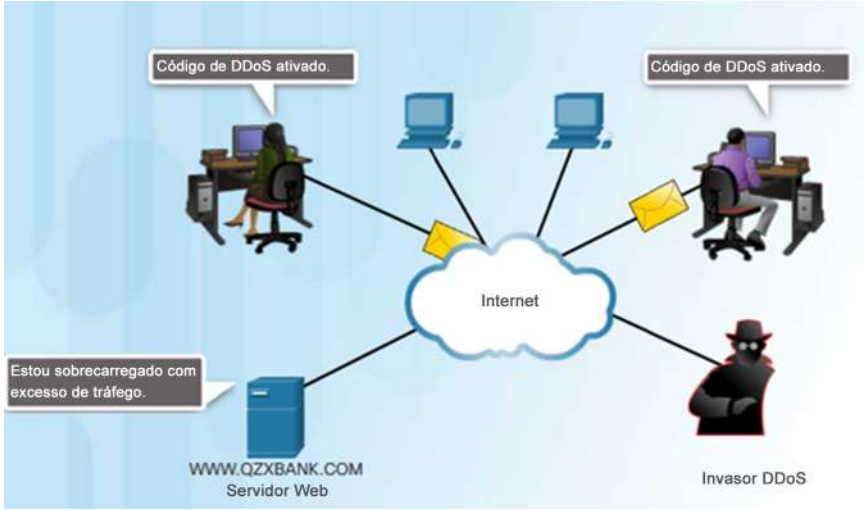
- DoS é uma interrupção de serviços de rede
  - **Grande quantidade de tráfego** – uma rede, host ou aplicativo recebe uma enorme quantidade de dados a uma taxa que não consegue processar.
  - **Pacotes formatados de forma mal-intencionada** – um pacote formatado de forma mal-intencionada é enviado para um host ou aplicativo e o receptor não consegue contê-lo.



Negação de serviço

DDoS

- Semelhante à DoS, de várias origens coordenadas
- Botnet – uma rede de hosts infectados
- Zumbi – hosts infectados
- Os zumbis são controlados por sistemas de tratamento.
- Os zumbis continuam a infectar mais hosts, criando mais zumbis.



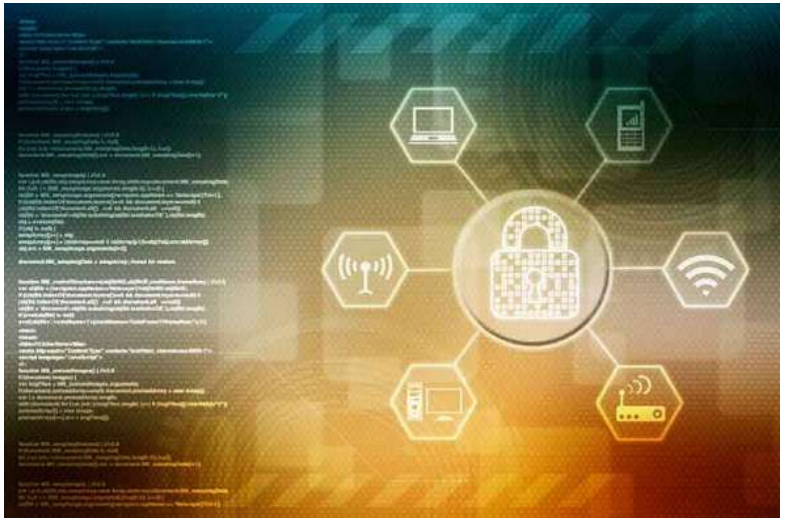
Envenenamento de SEO

- SEO
  - Otimização do mecanismo de pesquisa
  - Técnicas para melhorar o ranking de um site por um mecanismo de pesquisa
- Envenenamento de SEO
  - Aumenta o tráfego para sites mal-intencionados
  - Força os sites mal-intencionados a terem uma classificação mais alta

2.2 O mundo da segurança cibernética

O que é um ataque misto?

- usa várias técnicas para comprometer um alvo
- Usa um híbrido de worms, Cavalos de Troia, spyware, keyloggers, spams e esquemas de phishing
- Exemplo comum de ataque misto
  - mensagens de e-mail de spam, mensagens instantâneas ou sites legítimos para distribuir links
  - DDoS combinada com e-mails de phishing
- Exemplos: Nimbda CodeRed, BugBear, Klez, Slammer, Zeus/LICAT e Conficker



O que é redução do impacto?

- Comunicar a questão
- Ser sincero e responsável
- Fornecer detalhes
- Compreender a causa da violação
- Tomar medidas para evitar outra violação semelhante no futuro
- Certificar-se de que todos os sistemas estejam limpos
- Orientar os funcionários, parceiros e clientes

2.3 Resumo do capítulo

Resumo

- Identificar exemplos de vulnerabilidade da segurança.
- Explicar como uma vulnerabilidade da segurança é explorada.
- Descrever os tipos de malware e seus sintomas, métodos de infiltração, métodos usados para negar o serviço.
- Descrever um ataque misto e a importância da redução do impacto.


CISCO